IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: A GRAY APPLE IPHONE	Magistrate No. 24-1619

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, Kristen Luthy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—digital devices—which is currently in law enforcement possession (the "Device"), as described in Attachment A, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since April 2022, and was previously employed by the FBI since 2018 as an Investigative Specialist. As a Special Agent (SA) with the FBI, I am assigned to the Mon Valley Resident Agency, a satellite office, within the FBI's Pittsburgh Division. Within the Mon Valley Resident Agency, I am a member of the Southwest Pennsylvania Safe Streets Task Force. In this capacity, I am charged with investigating possible violations of federal criminal law. As a Special Agent with the FBI, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516. To become a Special Agent, I

successfully completed the FBI's Basic Field Training Course located in Quantico, Virginia. During my time in the FBI, I have also completed the FBI's Evidence Response Team Basic Course. While employed by the FBI, I have assisted with investigations into various violations, as well as participated in the execution of numerous search warrants, including but not limited to the following violations: domestic terrorism, international terrorism, cybercrimes, violent gangs, drug trafficking organizations, human trafficking, child exploitation and/or child sexual assault material (CSAM). During the course of conducting these investigations, I have been involved in the use of the following investigative techniques, to include but not limited to: interviewing informants and cooperating witnesses, conducting physical surveillance, obtaining and reviewing documentary and electronic evidence, and preparing and executing search warrants which have led to seizures of firearms, contraband, and evidence of criminal activity.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to search the Device, as there is reason to believe the device may contain evidence of a crime, further described below and in Attachment A, for the things described in Attachment B.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is a gray iPhone (FBI Evidence Item number 1B3), that is hereinto referred to as the "Device." The device was originally seized on July 19, 2023 from the home of Steven ONDULICH ("the Subject") during the execution of search warrant 23-mj-1198.

The device was not able to be downloaded at that time due to the technological capabilities of the FBI's digital device examiners at the time. On November 15, 2023, your Affiant received a signed search warrant to search three devices of ONDULICH, to include the above-mentioned Device for evidence of possible firearms violations. At this time, the Device was still not able to be downloaded to the passcode not being provided. On August 21, 2024, a passcode for the device was provided to your Affiant. Due to the passcode being provided, the FBI's digital device examiners are now able to download the device. Therefore, your Affiant is requesting a new search warrant in order to download and search the device. The Device is currently located at the FBI Pittsburgh Field Office, 3311 East Carson Street, Pittsburgh, Pennsylvania 15203.

PROBABLE CAUSE

Actions of Stephen ONDULICH on January 6, 2021:

6. Shortly after January 6, 2021, the FBI received a tip to its National Threat Operations Center that Stephen ONDULICH admitted to being at the U.S. Capitol that day. The FBI consequently found evidence that Stephen ONDULICH had participated in the January 6th U.S. Capitol Riots and had entered the Capitol.

Arrest of ONDULICH and Search of his Residence

7. On July 17, 2023, the government obtained an arrest warrant for ONDULICH from the U.S. District Court for the District of Columbia, (See Case No. 1:23-mj-00172) for violations of 18 U.S.C. §1752(a)(1), 18 U.S.C. §1752(a)(2), 40 U.S.C. §5104(e)(2)(D) and 40 U.S.C. §5104(e)(2)(G). On July 18, 2023, the government obtained a search warrant in the Western District of Pennsylvania (See Case No. 23-mj-1198) for ONDULICH's residence located at 216 1st Street, Unit 1, Trafford, Pennsylvania ("PREMISES"). Prior to the issuance of both warrants,

ONDULICH's residency at the PREMISES, had been confirmed via physical observations made by law enforcement officers.

8. While verifying ONDULICH's residency, law enforcement officers learned that ONDULICH was previously convicted of Second-Degree Assault and Stalking (See Case No. 6D00304800, Montgomery County District Court). The penalty for those charges carries a sentence of not more than three (3) years, thereby placing him in a "prohibited possessor" status federally, including in the states of Maryland and Pennsylvania. The date of the conviction was August 18, 2014, which occurred well before ONDULICH was known to the FBI.[1]

9. On July 19, 2023, both search and arrest warrants were executed at the PREMISES and ONDULICH was subsequently arrested by law enforcement officers. Upon his arrest, ONDULICH was provided with his Advice of Rights, which he signed and waived. Following his waiver of rights, ONDULICH was transported to the Pittsburgh Division Field Office and interviewed.

10. Stephen ONDULICH consequently plead guilty to Disorderly and Disruptive Conduct in a Restricted Building and Grounds in violation of 40 U.S.C. § 5104(e)(2)(D) and Parading, Demonstrating, or Picketing in a Capitol Building, in violation of 40 U.S.C. § 5104(e)(2)(G) regarding his participation in the breach of the U.S. Capitol on January 6th, 2021.

[1] Law enforcement officers obtained a certified copy of conviction on July 6, 2023. The prohibiting factors in the state of Maryland are further described in Maryland Public Safety Code 5-133 and 5-205. The prohibiting factors in the state of Pennsylvania are further described in Pennsylvania State Code 6105(b), which in this case, pertain to the conviction of Stalking in addition to that of Second Degree Assault.

Interview of Stephen ONDULICH

11. During ONDULICH's interview on July 19, 2023, he discussed his hobbies, which included building Privately Made Firearms ("PMFs"). ONDULICH was then confronted with the below conversation that was taken from his Instagram account with username *06_war_wagon*:

316	2021-03-22	**Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:11:48 UTC **Body** Hey man **Author** 06_war_wagon (Instagram: 202164064) **Sent** 2021-03-22 13:12:10 UTC **Body** Whats good man? **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:13:11 UTC **Body** I heard from a little bird. That you guys are making AR lowers? Lmao **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:13:23 UTC **Body** I'm here at your house doing work. 😂 It came up in conversation 😂 **Author** 06_war_wagon (Instagram: 202164064) **Sent** 2021-03-22 13:13:33 UTC **Body** Hahah you talk to josh? **Author** 06_war_wagon (Instagram: 202164064) **Sent** 2021-03-22 13:13:35 UTC **Body** 🤣🤣 **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:14:14 UTC **Body** Actually it was your dad that mentioned it. 😂 **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:14:18 UTC

		Body Last time I was here **Author** 06_war_wagon (Instagram: 202164064) **Sent** 2021-03-22 13:14:32 UTC **Body** Hahaha yeah man fuck biden and Harris but ya haven't made mine yet **Author** 06_war_wagon (Instagram: 202164064) **Sent** 2021-03-22 13:14:45 UTC **Body** But gov doesn't need to know what we have or possess **Author** 06_war_wagon (Instagram: 202164064) **Sent** 2021-03-22 13:14:48 UTC **Body** 🤣🤣🙏 **Author** 06_war_wagon (Instagram: 202164064) **Sent** 2021-03-22 13:15:03 UTC **Body** But yeah man got the stuff just gotta put it all together one Weekend ... **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:17:38 UTC **Body** Could I rent that Jig from you? 😂 😂 😂 😂 I have 3 lowers I need to machine out. I have a drill press and machines at my house lol ... **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:38:13 UTC **Body** I am gonna build 3 ARs for myself **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:38:23 UTC **Body** And I have 2 more for some friends of mine I gotta build **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:38:32 UTC **Body** And then I have a few other people that wanted to make one too **Author** ondulich787 (Instagram: 276604585) **Sent** 2021-03-22 13:38:36 UTC **Body** So I'm gonna be busy. 😂

12. After reviewing the transcript of the messages, ONDULICH admitted to participating in the conversation, but denied that any firearm transactions took place. ONDULICH further explained that many people had come to him requesting PMFs because of his skill in machining. Based on my training, knowledge and experience, I know that the term "AR" stands for ArmaLite Rifle. The term AR typically is used to describe an AR-15 style semi-automatic rifle based on or similar to the Colt AR-15 design. I also know that a fair degree of skill with machining and lathing is required in order to produce functional PMFs. Furthermore, I know that individuals who manufacture PMFs use pre-fabricated "jigs" on unfinished lower receivers in order to drill out the necessary holes and marks required to create a functional firearm. As it relates to the above

conversation, the term "jig" refers to a prefabricated guide that directs the user to drill and machine out holes and gaps in unfinished or "80-percent" lower receivers. The term "lower-receiver" refers to the lower portion of a rifle that houses the trigger and its components. According to the Gun Control Act of 1968 ("GCA"), a lower receiver is considered a firearm when it has been fully machined out and the part necessary to cause the expulsion of a projectile are added.

Items Recovered from ONDULICH's Residence

13. During the execution of the federal search warrant of the PREMISES, a subsequent state search warrant was issued for the PREMISES and the known white Honda Pilot bearing Maryland license plate 127M526, hereinafter referred to as VEHICLE. During the search of the RESIDENCE, twelve (12) fully assembled firearms were recovered, seven (7) of which did not have serial numbers. Ten (10) of the recovered firearms were found in either ONDULICH's bedroom, VEHICLE, or in the common living room space of the RESIDENCE. Of the twelve (12) firearms recovered, six (6) were completed AR-15 style rifles. Additional items recovered were one (1) "Daniel Defense" upper receiver and barrel, one silver upper and lower receiver (separate) assembly, one (1) black, lower receiver and various amounts of live ammunition for both rifles and pistols. Also located in the common living room space of the RESIDENCE was a UPS Ground package containing one (1) AR lower jig system. The UPS Ground package was from Tactical Gear Heads, and the shipping label had an unknown third-party individual with a Virginia address listed as the party the item was shipped to.

Observations Made During the Initial Review of ONDULICH's Gmail Account

14. The files provided by Google LLC. in response to the previously obtained search warrant (See case No. 23-SC-1173) were provided in compressed files, causing the viewer to "un-zip" the files and navigate to subfolders in order to view the media contained therein. Often, the

files were identified by numbers in the form of dates and identification numbers proprietary to Google LLC. Because the files were labeled in this manner, anyone reviewing the files would be required to open them and review the contents in order to further determine the relevancy of the objects contained therein.

15. In searching the returns from the Google LLC search warrant for media relevant to the events of January 6, 2021, investigators observed photographs and video seemingly depicting ONDULICH manufacturing using jigs, drill bits, and drill presses, possessing, and distributing PMFs. Many of the media files contained images of ONDULICH personally firing firearms, some of which are fully automatic[2], as well as photographs of finished and unfinished lower receivers, and those in the process of being "machined out."

16. The United States is now seeking this additional warrant, out of an abundance of caution, to seize information from the DEVICE related to our illegal firearms investigation being conducted out of the Western District of Pennsylvania. Thus, the United States seeks this warrant to authorize the search of the Device for evidence pertaining to ONDULICH's illegal manufacture and possession of firearms as further described in Attachment B.

TECHNICAL TERMS

17. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

[2] In this case, the term "fully automatic" is being used in the context of observing multiple shots being fired from a firearm with the single depression of the firearm's trigger.

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part

through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or

locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the

Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users

running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the

name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

18. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Devices, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Devices for at least the following reasons:

a. Individuals who engage in criminal activity, including the crimes associated with the illegal manufacture, possession and distribution of firearms, access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Devices, documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually

disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

19. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital Devices were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Devices at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular,

records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital Device are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device, not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs,

photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

20. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence

of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is

concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges,

content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

21. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic

examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Devices will be specifically chosen to identify the specific items to be seized under this warrant.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

22. Because forensic examiners will be conducting their search of the digital devices in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a warrant to search the Devices described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

s/ Kristen Luthy
Kristen Luthy
Special Agent
Federal Bureau of Investigation

Pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3), the undersigned judicial officer has on this date considered the information communicated by reliable electronic means in considering whether a complaint, warrant, or summons will issue. In doing so, I have placed the affiant under oath, and the affiant has confirmed that the signatures on the complaint, warrant, or summons and affidavit are those of the affiant, that the document received by me is a correct and complete copy of the document submitted by the affiant, and that the information contained in the complaint, warrant, or summons and affidavit is true and correct to the best of the affiant's knowledge.

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 30th day of September 2024.

_____
HONORABLE KEZIA O. L. TAYLOR
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is a gray iPhone (FBI Evidence Item number 1B3), that was found in the residence of Stephen ONDULICH (DOB: May 3, 1993) during the execution of a search warrant of ONDULICH's known residence located at 216 1st Street, Unit 1, Trafford, Pennsylvania 15085, hereinafter to be referred to as "PREMISES". The device (1B3) is currently located at the FBI Pittsburgh Field Office, 3311 East Carson Street, Pittsburgh, Pennsylvania 15203. The gray iPhone will hereinafter be referred to as "the device".

ATTACHMENT B

Property to be seized

1. The items, information, and data to be seized are fruits, evidence, information relating to, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. §§ 922(g)(1), Unlawful Possession of Firearm; § 922(a)(5), Transfer, sell, trade, give, transport, or deliver any firearm to any person who the transferor knows or has reasonable cause to believe does not reside in the State in which the transferor resides; § 922(d), Knowingly sell, give or dispose of firearm to any person who falls into the categories set forth in 922(g) and 922(n) as described in the search warrant affidavit, including, but not limited to:

a. Evidence concerning the unlawful manufacture and possession of firearms by persons prohibited under 18 U.S.C. §§ 922(g)(1);

b. Evidence of ONDULICH's awareness of his unlawful status of the possession of firearms.

c. Evidence of any transfer, sale, trade, give, transport, or delivery of any firearm to any person who the transferor knows or has reasonable cause to believe does not reside in the State in which the transferor resides as described in 18 U.S.C. §§ 922(a)(5);

d. Evidence concerning efforts to manufacture, possess and distribute unlawful firearms to others who meet the definition of unlawful possessors as described in 18 U.S.C. §§ 922(g) and 18 U.S.C. §§ 922(n);

e. Evidence relating to a conspiracy to illegally manufacture, possess and distribute unlawful firearms to others who meet the definition of unlawful possessors as described in 18 U.S.C. §§ 922(g) and 18 U.S.C. §§ 922(n) and others;

f. Evidence concerning communications about the illegal manufacture, sale or possession of firearms by or to persons prohibited by 18 U.S.C. §§ 922(g)(1).

g. Evidence concerning after-the-fact efforts to conceal evidence of those offenses, or to flee prosecution for the same;

h. Evidence of the state of mind of the Subject and/or other co-conspirators, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience related to the criminal activity under investigation; and

i. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under

investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

j. Evidence of who used, owned, or controlled the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

k. Evidence of software, or the lack thereof, that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

l. Evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;

m. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Devices;

n. Evidence of the times the Devices were used;

o. Passwords, encryption keys, and other access devices that may be necessary to access the Devices;

p. Documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices;

q. Records of or information about Internet Protocol addresses used by the Devices;

r. Records of or information about the Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.